MCLE ON THE WEB ($15 PER CREDIT HOUR)
TEST #23
1 HOUR CREDIT
LEGAL ETHICS

To earn 1 hour of MCLE credit in the special category of Legal Ethics, read the substantive material, then download the test, answer the questions and follow the directions to submit for credit.

Corporate Counsel Beware
Economic espionage is on the rise, creating an ethical, and potentially criminal quagmire

By RUSSELL L. BOLTWOOD
and FELIX L. FISCHER

Consider the following: The CEO of the biotech company you represent has just finished a very successful presentation to analysts and investors in attendance at an industry conference highlighting emerging companies. She makes the rounds of the hospitality suites and appears at the reception desk of one of her customer's suites for a meeting later that day.

Not surprisingly, executives of some of the other emerging biotech companies represented at the conference are in and about the suite. As the receptionist calls her for her private meeting, your CEO notices (quite innocently) a manila folder file left behind in an empty seat.

The word "Confidential" is written on a yellow post-it note, which is attached to the front of the file. Without thinking about who the file might belong to, or what its contents may be, your CEO opens the folder. Very quickly, she discovers she's looking at the strategic market plan and projected inventory data for one of her company's fiercest competitors.

Or consider this: After seemingly endless months of wooing and negotiations, a leading engineering executive finally agrees to join your client company in the capacity of Chief Technology Officer. Although the new CTO was an executive at a competing firm, you feel confident that the the existing regimen of pre-employment agreements and policy provisions provided by you to your client will more than adequately protect your client from allegations of trade secret misappropriation related to the hiring of the CTO.

Or a condition often experienced by members of a development team's technical engineering staff: The project manager for your client's customer invites your client's chief engineer into the customer's test laboratory to see a prototype device being quickly developed to compete with a similar device by rival Company X. The prototype device sits side-by-side in the lab with the Company X device. The project manager confides in your chief engineer, stating, "You've been our preferred supplier and we'd like to continue doing business with you. But, as you can see, the metallic Unobtainium coating on Company X's product makes it run much more efficently, with double the product life. If you could just add the coating to your device, you'd probably get similar performance."

Could any of these scenarios be the seeds of federal criminal liability?

With the advent of the Economic Espionage Act of 1996 (EEA), the answer would be yes — with potentially serious consequences for both your client company and its officers. The purpose of this article is to provide corporate counsel with some general background as to the history of trade secret jurisprudence, the effect of the EEA on existing trade secret law, and steps that corporate counsel may take to mitigate the possibility of corporate and individual liability under the EEA.

The rise of economic espionage

Economic espionage is on the rise, both as a purely domestic matter, and also as between international parties. For example, a survey released in 1996 by the American Society for Industrial Security showed a 323 percent increase in incidents from 1992 to 1995. The FBI also reported that during the late 1990s, at least 23 foreign governments were then stealing (or attempting to steal) intellectual assets from U.S. corporations.

This trend is not surprising when viewed in the context of recent historic and technological developments. The end of the Cold War has led governments to shift the focus of their espionage efforts from military to industrial matters.

Additionally, the rising importance of intellectual property to the global economy has led to a growing shift from industrial crimes involving tangible property to those targeting intellectual property.

Finally, the advent of e-mail and the Internet has increased the ease and speed with which valuable intellectual property assets can be misappropriated.

Put together, these factors suggest that trade secret misappropriation and associated intellectual property crimes will only continue to grow in economic magnitude and public visibility.

A brief history

Trade secret law can trace its origins to commercial transactions, more specifically to the implied duty of good faith that developed at common law in regard to commercial dealings.

Historically, courts protected the owner of a trade secret when another party had employed improper means to learn the trade secret, most often holding that the misappropriator of the secret had breached his "duty of good faith" with respect to the commercial relationship. Under early California case law, the unauthorized use or disclosure of another's trade secret was normally actionable as a breach of confidence, as opposed to bring actionable as a violation of a property right. See, e.g., Riess v. Sanford (1941) 47 Cal.App.2d 244.

Typically, the definition of "trade secret" at common law focused narrowly on the nature of the protected information per se. For example, in Sinclair v. Aquarius Electronics, Inc. (1974) 42 Cal.App.3d 216, the First District Court of Appeal defined "trade secret" as:

". . . any formula, pattern, device or compilation or information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."

Compare California's common law definition of "trade secret" with that contained within the Restatement (Fourth) of Torts (1939): ". . . any formula, pattern, device, or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers." The Restatement's definition is arguably narrower than that at California common law, as it appears to focus more narrowly on technical or engineering information, as opposed to a broader and more generalized notion of "business information."

The narrow nature of common law definitions of "trade secret" failed to address important characteristics of trade secrets which were often an important point of contention between litigants, such as whether the trade secret should possess actual and current economic value to be granted protection (as opposed to perceived future value), or what level of protection a trade secret should be given by its owner for the courts to recognize the actual existence of a trade secret. As such, the narrow scope of common law definitions of "trade secret" often proved less than adequate for application by the courts to particular cases, or for use by corporate counsel to provide guidance to clients as to what would or would not constitute trade secret misappropriation.

The Uniform Trade Secrets Act

The promulgation of the Uniform Trade Secrets Act (UTSA) in 1979 attempted to resolve the above-described definitional issues, while at the same time substantially broadening the definition of what constitutes a "trade secret." As adopted by the California legislature in 1984 and codified at California Civil Code §3426 et. seq., "trade secret" is defined by the UTSA as:

". . . information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (a) derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." Cal. Civ. Code §3426.1(d).

The UTSA definition broadened the scope of common law trade secret protections by covering those secrets which may possess only potential value to the holder, while at the same time narrowing the scope of protection to those trade secrets for which efforts "reasonable under the circumstances" had been made by the holder to protect the secret's confidentiality.

Despite the improvements provided by the UTSA over common-law formulations of trade secret law, the UTSA approach has proved inadequate in several important respects. First, the state-by-state approach envisioned by the promulgation of the UTSA has led to significant distinctions between states in terms of the evolution of trade secret jurisprudence, as each state's judicial interpretation of the UTSA has been necessarily colored by existing state decisional law. (Although such state-by-state distinctions are too numerous for analysis within the scope of this article, the authors recommend the excellent analysis at §1.01[3] of Milgram, Trade Secrets (1999 edition).

Second, the UTSA failed to define what medium of expression a given trade secret must take in order to rise to the level of protection envisioned by the UTSA, as well as to properly evidence the owner's intent to maintain confidentiality.

Finally, the UTSA approach had been effectively outstripped by the above-described historical and technological developments, particularly with respect to its unsuitability as a tool to discourage and punish economic espionage between international actors.

The new federal law

The Economic Espionage Act was signed into law on Oct. 11, 1996, and is codified at 18 USC §1831 et seq. Section 1831 of the EEA applies to misappropriation of trade secrets by those intending to benefit any foreign government (which includes virtually any individual, corporate entity, or government agency acting on behalf of a foreign government); however, this provision does not require that the trade secret be related in some way to a product, or that the owner of the trade secret suffer actual injury. An individual who misappropriates trade secrets under §1831 is subject to a fine of not more than $500,000 and/or imprisonment of not more than 15 years. 18 USC §1831(a). An organization that commits such an offense is subject to a fine of not more than $10 million.

Section 1832 prohibits any individual or entity from misappropriating trade secrets with the intent to convert the trade secret to the economic benefit of another, or furthering such an act, or attempting or conspiring to do so. Unlike §1831, §1832 does not require an intent to benefit a foreign government. Further, §1832 is only limited as protecting trade secrets "related to or included in a product that is produced for or placed in interstate or foreign commerce." However, it must be proved that it was intended or known that injury to the trade secret owner would occur as a result of the misappropriation. An individual committing such an offense can be fined and/or imprisoned for not more than 10 years. 18 USC §1832(a). Any such organization can be fined not more than $5 million.

Of no small significance, the EEA also contains substantial and potentially far-reaching forfeiture provisions. In addition to its provisions for imprisonment and fines, the EEA also requires that the sentencing court "shall order" forfeiture to the United States of "any property" constituting or derived from proceeds obtained as the result of the violation. 18 USC §1834(a)(1). Section 1834 (a)(2) further permits the court, "in its discretion," to order forfeiture of "any of the person's property used, or intended to be used . . . to commit or facilitate the commission of such violation," in addition to the proceeds.

The EEA's definition

In contrast to both common law and UTSA-based definitions of "trade secret," the definition offered by the EEA substantially broadens what may constitute a "trade secret." Also unlike the UTSA, the EEA also defines what media of expression a "trade secret" may take to in order to fall within the statute's ambit.

The EEA defines "trade secret" as ". . . all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public . . ." 18 USC §1839(3).

Two points are worth noting about the breadth of the EEA's definition of "trade secret." The act covers a broad range of information categories, such as financial and business information; many of these categories do not fall within most companies' traditional view of what constitutes a "trade secret." Additionally, the definition's inclusion of trade secrets ". . . whether tangible or intangible, and whether or how stored, compiled or memorialized . . ." potentially poses significant problems for companies, particularly with respect to the recruitment and hiring of new employees. Referring back to the second hypothetical situation above, even the CTO's personal memories and recollections of his prior employer could arguably raise the specter of criminal liability for his new employer under the EEA.

Civil misappropriations

As of the date of this article, criminal prosecutions under the EEA have been few. Through 1999, there had been 11 cases brought under the EEA by the federal government; six have resulted in guilty pleas. However, the current paucity of enforcement activity may ultimately prove to be misleading, especially in light of the EEA's potential impact on civil trade secret misappropriation disputes.

With its specific criminalization of trade secret theft, the advent of the EEA raises the possibility that trade secret owners contemplating or engaging in civil litigation over alleged trade secret theft may request the assistance of the federal government in investigating the alleged theft. Presuming that the government would choose to intervene, its powers of search and seizure could be indirectly employed to produce incriminating evidence otherwise subject to civil discovery procedures.

A company which chooses to resist such "forced discovery" would arguably run the risk of being charged with criminal obstruction of justice. Presuming further that a criminal trial results from such an investigation, a trial would serve to reveal a defendant's case strategy, strengths and weaknesses. Moreover, a conviction pursuant to the higher burden of proof applicable to a criminal trial proceeding would likely mean the existence of sufficient proof for liability under the less stringent burden of proof applicable to civil cases.

Indeed, the mere undertaking of a criminal investigation by the federal government, with its attendant negative publicity, could lead to very serious consequences for the alleged misappropriator and its relationships with customers, suppliers, creditors, employees and investors. As such, it would seem that the potential for criminal indictment under the EEA may induce a party who has misappropriated trade secrets to settle privately and on favorable terms with the owner of an assorted trade secret.

Minimizing your client's exposure

As described above, the EEA presents a new and potentially potent force in the context of trade secret litigation. Of course, such litigation most often arises where actual wrongdoing has occurred; the vast majority of companies act ethically and responsibly with respect to the "care and handling" of trade secrets. However, because of the expansive reach of the EEA, even those companies with outstanding ethics and compliance practices can find themselves unknowingly exposed to criminal liability.

Scenarios, such as our three examples, that previously would have been insignificant in the civil litigation context as an inadvertent discovery or potentially a breach of a confidentiality agreement by a third party, now may result in an attempt, conspiracy or actual perpetration of an offense under the EEA, if the confidential nature of information is known and it is used in any commercial manner to the detriment of the owner.

Criminal liability via the EEA is particularly insidious because it may arise through many otherwise routine activities of an enterprise, such as hiring employees or independent contractors, dealing with suppliers or customers, or entering into new business relationships as either investor or subject of investment.

Any of these activities is a potential touchstone of liability under the EEA; indeed, as the first hypothetical above suggests, even the seemingly innocent act of sending employees to an industry conference creates situations which might lead to liability. Therefore, it is important for companies to be aware of the EEA's provisions and to protect themselves from EEA liability.

The following list suggests in general terms those actions corporate counsel should consider taking to protect their clients from EEA liability:

1. Develop and promulgate a written policy that applies the provisions of the EEA to the specifics of your client's business. At a minimum, the policy should:

Outline the basic provisions and penalties of the EEA;

Give specific examples of where EEA liability may arise, based upon your client's most frequent business activities;

Provide meaningful advice as to avoiding EEA liability; and

Advise as to consequences of intentional disobedience of the policy.

The policy should be incorporated in both your client's employee handbook and its financial policies and procedures manual. Additionally, the policy should be the subject of regular training for your client's employees, as well as a subject matter for your client's internal audit function.

2. With respect to new employees, ensure that an appropriate employment agreement is signed by the employee at the inception of their employment which advises them of the existence of the EEA, their duty to abide by its provisions, and the consequences to their employment for failing to do so. Well-drafted agreements will advise new employees that they may possess trade secrets of previous employers, and that they are not to use or disclose such information in connection with their work for your client company.

3. Individuals retained by your client as independent contractors (consultants) should also be required to sign an agreement at the inception of their relationship with your client that is similar to the agreement for new employees, as described above. In the case of independent contractors, the agreement should also include provisions that require the contractor to indemnify the client company in cases where civil EEA liability is derived from the independent contractor's acts or omissions.

4. Provisions relating to the EEA should also be included in your client company's standard contracts for vendors and customers. Well-drafted EEA provisions will also require a vendor or customer to indemnify your client company where their actions or omissions have caused the company civil EEA liability.

5. Non-disclosure agreements used by your client at the inception of potential commercial dealings with another party should be modified to include provisions covering the EEA, with indemnification provisions if deemed appropriate.

6. The importance of proper marking and handling of documents (as well as any other tangible medium of record) as "proprietary and confidential" must be emphasized to the cli-ent's officers and employees, if for no other reason than the protection offered by the EEA for information which the client has taken reasonable measures to keep secret.

7. Operating procedures for dealing with customers and competitors should be established to prevent client personnel from having to guess how to receive and treat information, with special attention to provisions for a "good faith" response if confidential information is inadvertently obtained or received. Such a "good faith" response may serve to defeat the "intent" requirement of the EEA.

8. Finally, be sure you fully understand the corporate structure of your client, particularly with respect to companies which do a substantial amount of international business. Countries with emerging or post-Communist economies often require foreign businesses to form joint ventures or minority-owned subsidiary companies with internal governmental entities in order to do any business within the country. Such business forms are a potential wellspring of EEA liability because of the established legal relationship between your client and a foreign government.

In sum, the EEA is at present a new, little-enforced federal criminal statute, with little history in terms of either prosecution or litigation. However, the increasing importance of trade secrets within the global economy make clear that the EEA will likely become a prominent enforcement tool for the federal government in the near future. Corporate counsel would be wise to study its provisions and implement compliance safeguards now, rather than risking the uncertainty of potential criminal liability in the future.

Russell L. Boltwood is corporate counsel and human resources director for a California-based telecommunications equipment provider. Felix L. Fischer is group general counsel and chief patent counsel for Honeywell International.

Test — Legal Ethics
1 Hour MCLE Credit

This test will earn 1 hour of MCLE credit in Legal Ethics.

1. True/False. At common law, most courts remedied trade secret misappropriation under the doctrine of the implied duty of good faith in regard to commercial dealings.

2. True/False. Common law trade secret jurisprudence specifically required that a trade secret possess actual and current economic value in order to receive judicial protection.

3. True/False. Prior to the promulgation of the Uniform Trade Secrets Act (UTSA), trade secret law was a subject of both state and federal common law.

4. True/False. The UTSA's definition of "trade secret" broadened the scope of common law trade secret protections by covering those secrets which may possess only potential value to the holder.

5. True/False. The Economic Espionage Act (EEA) applies to misappropriation of trade secrets by both governmental and private entities.

6. True/False. EEA liability for private entities requries a showing that the misappropriator of a trade secret intended to injure the trade secret holder, or knew that injury to the trade secret holder would occur because of the misappropriation.

7. True/False. Individuals found liable under the EEA may be subject to imprisonment of not more than 15 years.

8. True/False. The EEA requires that when passing sentence on a proven EEA violation, the sentencing court shall also order forfeiture to the United States of any property constituting or derived from proceeds obtained as a result of the violation.

9. True/False. The EEA protects trade secrets from misappropriation even if the owner has not taken any steps to keep the trade secret confidential.

10. True/False. Under the EEA, trade secret protection is limited to scientific and technical information.

11. True/False. The EEA creates a private right of action for civil litigants involved in trade secret misappropriation actions.

12. True/False. Potential criminal liability under the EEA is specifically limited to trade secret misappropriation occurring in the context of dealings between commercial customers and suppliers.

13. True/False. Liability for trade secret misappropriation, if proven under the EEA, would likely mean the existence of civil liability for trade secret misappropriation.

14. True/False. The EEA, although a relatively new federal statute, has been widely litigated.

15. True/False. To mitigate potential EEA liability, a company should advise new employees at the inception of their employment of the EEA's provisions and the employee's duty to abide by such provisions.

16. True/False. Independent contractors to a company may indemnify the company from EEA criminal liability.

17. True/False. The EEA creates a rebuttable presumption that a company's trade secrets are protected by the statute, meaning that a company need not bother with taking steps to specifically identify trade secret materials as proprietary and confidential.

18. True/False. Only companies with foreign subsidiaries need be concerned about potential criminal liability under the EEA.

19. True/False. Inadvertent receipt of confidential information does not implicate potential liability under the EEA.

20. True/False. Companies should make the EEA a regular subject of employee training, as well as a subject for review by the company's internal audit function.

Certification

- This activity has been approved for Minimum Continuing Legal Education credit by the State Bar of California in the amount of 1 hour, of which 1 hour will apply to Legal Ethics.

- The State Bar of California certifies that this activity conforms to the standards for approved education activities prescribed by the rules and regulations of the State Bar of California governing minimum continuing legal education.

MCLE ON THE WEB
TEST #23 – Corporate Counsel Beware
1 HOUR CREDIT
LEGAL ETHICS

- Print the **answer form only** and answer the test questions.
- Mail **only form and check** for $15 to:

MCLE on the Web
The State Bar of California
Attn: Ibrahim Bah
180 Howard Street
San Francisco, CA 94105

- Make checks payable to State Bar of California.
- A CLE certificate will be mailed to you within eight weeks.

_____
Name

_____
Law Firm/Organization

_____
Address

_____
State/Zip

_____
State Bar Number (Required)

1.	TRUE ____	FALSE _____	11.	TRUE ____	FALSE _____
2.	TRUE ____	FALSE _____	12.	TRUE ____	FALSE _____
3.	TRUE ____	FALSE _____	13.	TRUE ____	FALSE _____
4.	TRUE ____	FALSE _____	14.	TRUE ____	FALSE _____
5.	TRUE ____	FALSE _____	15.	TRUE ____	FALSE _____
6.	TRUE ____	FALSE _____	16.	TRUE ____	FALSE _____
7.	TRUE ____	FALSE _____	17.	TRUE ____	FALSE _____
8.	TRUE ____	FALSE _____	18.	TRUE ____	FALSE _____
9.	TRUE ____	FALSE _____	19.	TRUE ____	FALSE _____
10.	TRUE ____	FALSE _____	20.	TRUE ____	FALSE _____